UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

JILLIAN CANTINIERI, individually, and on behalf of all others similarly situated,

Plaintiff,

v.

VERISK ANALYTICS, INC., INSURANCE SERVICES OFFICE, INC., and ISO CLAIMS SERVICES INC.

Defendants.

Civil Action No.: 2:21-cv-6911

CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED

JILLIAN CANTINIERI ("Plaintiff"), individually, and on behalf of all others similarly situated, by and through her undersigned counsel, hereby submits the following Class Action Complaint and Demand for Jury Trial against VERISK ANALYTICS, INC., INSURANCE SERVICES OFFICE, INC., and ISO CLAIMS SERVICES INC. (collectively, "Defendants") and alleges the following upon information and belief:

NATURE OF THE ACTION

1. Plaintiff, individually, and on behalf of all others similarly situated, brings this proposed class action against Defendants seeking damages for actual and imminent or impending injuries as a result of Defendants' negligent failure to safeguard the personally identifiable information ("PII") of Plaintiff and the members of the proposed classes from a targeted breach of its databases ("data breach") by unauthorized entities or criminals.

2. Defendants own and maintain databases containing billions of detailed insurance claim records and PII, and each year collect tens of millions more individual claim records from insurers and other participating users. Defendants' "flagship" database, the ISO ClaimSearch

database, is the largest claims database in the world, and provides claim reports to insurers, brokers, actuaries, government entities, and law enforcement agencies, among others, for claims investigation and research purposes. In addition to insurance claim information, Defendants also directly and indirectly acquire and maintain the PII of the claimants in its databases, including full names, addresses, telephone numbers, vehicle identification numbers ("VIN), license plate numbers, driver's license numbers, tax identification numbers ("TIN"), and Social Security numbers ("SSN").

3. Upon information and belief, as early as July 5, 2021, and potentially earlier, unauthorized entities or criminals exploited the weaknesses and vulnerabilities in Defendants' data security systems, infiltrated their databases, and exfiltrated and exposed massive amounts of individual claimant information, including the PII of Plaintiff and the members of the proposed classes. The data breach continued undetected for approximately three months, or potentially longer, when Defendants finally discovered unusual activity in their data systems. During that timeframe, Defendants negligently failed to identify or prevent the unauthorized breach of its data systems or safeguard the highly sensitive PII of Plaintiff and the members of the proposed classes with adequate and reasonable cybersecurity measures.

4. Defendants knew, or should have known, the importance of safeguarding highly sensitive PII on their data systems, as well as the foreseeable and natural consequences of a data breach. Defendants, however, failed to take adequate cybersecurity measures to prevent the data breach from occurring and, as a result, caused Plaintiff and the members of the proposed classes to suffer irreparable harm from identity theft, financial fraud, and loss of privacy.

5. Furthermore, the foreseeable ramifications of Defendants' negligent failure to keep the PII of Plaintiff and the members of the proposed classes secure are long-lasting and severe,

because many of data points in the compromised and exposed PII are persistent or permanent, such as SSNs or dates of birth. The reality is that criminals who have purchased, or will purchase, the PII belonging to Plaintiff and the members of the proposed classes exposed in the data breach do not need to immediately use the PII to commit fraud. Rather, these individuals can wait indefinitely to use or sell the subject PII at any later time. As such, Plaintiff and the members of the proposed classes remain at risk of identity theft, financial fraud, and loss of privacy for the rest of their lives.

6. Plaintiff and the members of the proposed classes have suffered actual and imminent or impending injuries as a direct and proximate result of Defendants' negligent failure to prevent or detect the data breach, including: (a) theft of their PII; (b) actual fraudulent activity on their financial accounts; (c) lowered credit scores resulting from credit inquires following fraudulent activity; (d) increased fraudulent phone calls and email phishing attempts; (e) costs associated with the detection and prevention of identity theft and financial fraud; (f) costs associated with time and the loss of productivity spent addressing and attempting to monitor, ameliorate, mitigate, and deal with the consequences of the data breach; (g) stress, nuisance, and annoyance from dealing with the consequences of the data breach; (h) imminent, impending, and increased risk of future identity theft and financial fraud posed by ill-intentioned unauthorized entities or criminals possessing their PII; (i) damages to and diminution in value of their PII; (j) the retention of the reasonable value of the PII still in Defendants' possession; and (k) the continued risk to their PII which remains in the possession of Defendants and is subject to further data breaches so long as Defendants fail to undertake appropriate and adequate cybersecurity measures.

7. Plaintiff, individually, and on behalf of all others similarly situated, seeks to remedy these injuries, prevent their future occurrence, and, accordingly, asserts claims for negligence,

negligence *per se*, unjust enrichment, violation of applicable federal and state statutes, including Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 and New York General Business Law ("New York Gen. Bus. Law") § 899-aa and § 349, and seeks monetary damages, injunctive relief, declaratory relief, and all other available relief by law or in equity.

THE PARTIES

PARTY PLAINTIFF

8. Plaintiff is a natural person and, at all relevant times, has been a United States citizen and resident of Nassau County, New York.

9. Upon information and belief, prior to the data breach, Plaintiff's insurer submitted certain automobile claim information to Defendants, and the claim information included, among other things, certain PII, including, but not limited to, Plaintiff's full name, address, date of birth, driver's license number, and SSN.

10. Upon information and belief, after Plaintiff's insurer submitted the aforementioned information to Defendants, and unauthorized entities or criminals exploited foreseeable weaknesses and vulnerabilities in Defendants' data security systems in a targeted data breach and obtained Plaintiff's PII.

11. Upon information and belief, the aforementioned unauthorized entities or criminals illegally accessed, obtained, exfiltrated, and exposed Plaintiff's PII in the data breach, exploited and misused her PII to commit identity theft or financial fraud, or released or sold her PII to other unauthorized entities or criminals to commit further or future acts of identity theft or financial fraud.

12. As a direct result of the data breach, Plaintiff suffered numerous incidents of identity theft and financial fraud without any knowledge her data had been compromised and without any notice from Defendants about the data breach or the risk of harm to her.

13. In November 2021, Plaintiff received a letter from Defendants, dated November 4, 2021, which notified her for the first time of the data breach and that her PII may have been compromised.

14. As a result of the data breach and its long-lasting and severe ramifications, Plaintiff has suffered actual harm from identity theft and financial fraud, as well as imminent and impending harm from future identity theft and financial fraud.

15. As a result of the data breach, Plaintiff has furthermore suffered, and will continue to suffer, from emotional anguish and distress, including, but not limited to fear and anxiety related to the exposure and exploitation of her PII and resulting vulnerability to imminent and impeding identity theft or financial fraud in the future.

16. Accordingly, Plaintiff asserts the foregoing action individually and on behalf of all other similarly situated.

PARTY DEFENDANTS

17. Defendant VERISK ANALYTICS, INC. ("VERISK") is a publicly traded Delaware corporation with its principal place of business located at 545 Washington Boulevard, Jersey City, New Jersey 07310-1686.

18. Upon information and belief, VERISK was established in 2008 as a Delaware Corporation by Defendant INSURANCE SERVICES OFFICE, INC. ("ISO") to function as ISO's parent holding company.

19. Upon information and belief, VERISK is the parent company of Defendant INSURANCE SERVICES OFFICE, INC. ("ISO").

20. Upon information and belief, at all relevant times, VERISK gathered, possessed, stored, organized, and maintained the PII of Plaintiff and the members of the proposed classes that was compromised and exposed in the data breach.

21. Upon information and belief, at all relevant times, VERISK was the owner, custodian, and steward of the databases containing the PII of Plaintiff and the members of the proposed classes that was compromised and exposed in the data breach.

22. Upon information and belief, at all relevant times, VERISK was responsible for the privacy and security of the PII of Plaintiff and the members of the proposed classes that was compromised and exposed in the data breach.

23. Upon information and belief, ISO is a Delaware corporation with its principal place of business located at 545 Washington Boulevard, Jersey City, New Jersey 07310-1686.

24. ISO was formed in 1971 as a voluntary, non-profit, unincorporated association of insurers through the consolidation of various state, regional, and national rating bureaus for various lines of property and casualty insurance.

25. ISO changed and became a for-profit corporation in 1997.

26. ISO established VERISK as a corporate entity in 2008 to serve as ISO's parent holding company, and ISO became a wholly-owned subsidiary of VERISK in 2009.

27. ISO is presently a wholly owned subsidiary of VERISK.

28. Upon information and belief, at all relevant times, ISO gathered, possessed, stored, organized, and maintained the PII of Plaintiff and the members of the proposed classes that was compromised and exposed to the data breach.

29. Upon information and belief, at all relevant times, ISO was the owner, custodian, and steward of the databases containing the PII of Plaintiff and the members of the proposed classes that was compromised and exposed in the data breach.

30. Upon information and belief, at all relevant times, ISO was responsible for the privacy and security of the subject PII of Plaintiff and the members of the proposed classes that was compromised and exposed in the data breach.

31. Upon information and belief, at all relevant times, Defendant ISO CLAIMS SERVICES INC. ("ISO CLAIMS") is a Delaware corporation with its principal place of business located at 545 Washington Boulevard, Jersey City, New Jersey 07310-1686.

32. ISO CLAIMS is a wholly owned subsidiary of ISO.

33. Upon information and belief, at all relevant times, ISO CLAIMS possessed, stored, organized, and maintained the PII of Plaintiff and the members of the proposed classes that was compromised and exposed in the data breach.

34. Upon information and belief, at all relevant times, ISO CLAIMS was the owner, custodian, and steward of the databases containing the PII of Plaintiff and the members of the proposed classes that was compromised and exposed in the data breach.

35. Upon information and belief, at all relevant times, ISO CLAIMS was responsible for the privacy and security of the subject PII of Plaintiff and the members of the proposed classes that was compromised and exposed in the data breach.

36. Upon information and belief, at all relevant times, Defendants were and are in the business of gathering, possessing, storing, organizing, and maintaining claim information and PII of claimants, including the PII of Plaintiff and the members of the proposed classes, to develop

data and analytics systems and services and sell access to those systems and services to subscribing customers.

37. Upon information and belief, at all relevant times, Defendants acted in concert in gathering, possessing, storing, organizing, and maintaining claim information and PII of claimants, including the PII of Plaintiff and the members of the proposed classes, to develop data and analytics systems and sell access to those systems and services to subscribing customers.

38. Upon information and belief, at all relevant times, Defendants combined their property and labor in a joint undertaking for profit with rights of mutual control over each other in gathering, possessing, storing, organizing, and maintaining claim information and PII of claimants, including the PII of Plaintiff and the members of the proposed classes, to develop data and analytics systems and services and sell access to those systems and services to subscribing customers.

39. Upon information and belief, at all relevant times, Defendants operated as a single enterprise, equally controlled each other's business affairs, commingled their assets and funds, disregarded corporate formalities, and used each other as corporate shields.

40. Upon information and belief, at all relevant times, Defendants acted as, and were, mere alter egos or instrumentalities of each other.

41. Upon information and belief, at all relevant times, there has been such a unity of interest and ownership between Defendants that the separate personalities of their respective entities ceased to exist.

42. Upon information and belief, at all relevant times, Defendants acted in all respects as agents or apparent agents of one another and, as such, are jointly liable to Plaintiff and the proposed class.

JURISDICTION AND VENUE

43. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) as the amount in controversy exceeds $5 million dollars, exclusive of interest and costs and, upon information and belief, the size of the proposed classes very likely numbers in the thousands, and potentially over millions, of individuals given the size and scope of Defendants' databases, more than two-thirds of whom have different citizenship than Defendants, including the Plaintiff named herein.

44. Also, through their business operations in this District, Defendants have intentionally availed themselves to the markets within this District such that exercising jurisdiction over Defendants by this Court is just and proper.

45. Furthermore, venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1), because a substantial part of the events giving rise to this action occurred in this District; a substantial part of property that is subject of the action is situated in this District; and because Defendants transact substantial business generally in this District.

FACTUAL ALLEGATIONS

A. Background – Data is at the Core of what Defendants do.

46. Defendants are among the largest global data aggregators and data analytics providers in the world.

47. Defendants primarily develop data analytics tools and programs to assist insurers and other customers in defining and managing risk and insurance products.

48. Defendants collect and analyze billions of records using advanced technologies and provide predictive data analytics and support solutions to customers in fields of rating,

underwriting, claims, catastrophe and weather risk, natural resources intelligence, economic forecasting, commercial banking and finance, and other fields involved in risk analysis.

49. Defendants' customers include all of the top 100 property and casualty insurance providers in the United States; the top 30 credit card issuers in North America, the United Kingdom, and Australia; 9 of the top 10 global energy producers; and a wide range of companies, governments, and institutions across energy, metals, and mining value chains.

50. Defendants' massive data sets include hundreds of millions of property and casualty insurance claims, historic natural catastrophe data from more than 50 countries, data from tens of millions of mortgage loan applications, and hundreds of millions of United States criminal records.

51. Defendants' anti-fraud data products include data on claim histories, analyses of mortgage applications to identify misinformation, analysis of prior claims to find emerging patterns of fraud and identification of suspicious claims in insurance, health care, and mortgage sectors.

52. Defendants' largest property and casualty insurance database is the ISO ClaimSearch database, which includes tens of billions of individual insurance records, with billions of new records added each year.

53. Defendants offer their data analytics services and support solutions to customers through annual subscriptions or long-term agreements.

54. Defendants' range of subscription services are also incredibly lucrative.

55. At the end of 2020, Defendants reported total revenue of over $2.7 billion dollars, of which, approximately 82% came from data analytics subscriptions and service agreements.

B. Defendants Allowed a Targeted Data Breach to go Unnoticed and Unimpeded.

56. On September 27, 2021, ISO CLAIMS reportedly detected unusual activity on a customer account within its network.

57. ISO CLAIMS determined at a later time that as early as July 5, 2021, an unauthorized entity had infiltrated its network in a targeted data breach and obtained the PII of Plaintiff and the members of the proposed classes.

58. ISO CLAIMS sent a letter to Plaintiff and, upon information and belief, the members of the proposed classes, dated November 4, 2021, disclosing to them for the first time of the data breach ("the Disclosure Letter"), stating:

> It appears an unauthorized entity obtain[ed] credentials to access [ISOC's] customer portal as early as July 5, 2021, and obtain [sic] certain motor vehicle reports containing driver names, dates of birth, addresses, and driver's license numbers.

59. ISO CLAIMS acknowledged in the Disclosure Letter that it had taken "multiple, further steps to reduce the risk of this type of an incident happening again…" However, upon information and belief, the scope of the timeframe during which ISO CLAIMS's networks remained compromised began much earlier than reported by ISO CLAIMS. Furthermore, upon information and belief, the scope of the PII released in the data breach was far more expansive than reported in the Disclosure Letter and included, but was not limited to, SSNs, prior names and addresses, copies of identification documents, and property and casualty claim information and reports pertaining to Plaintiff and the members of the proposed classes.

60. The Disclosure Letter advised that ISO CLAIMS had arranged for Plaintiff and, upon information belief, the members of the proposed classes, to obtain credit monitoring and identity protection services at no cost for up to two-years, and recommended that "[Plaintiff] remain vigilant and review [their] financial records and statements for signs of suspicious activity."

61. Nevertheless, ISO CLAIMS's offer of credit monitoring and identity protection services could not prevent the irreparable harm already suffered by Plaintiff at that time, or adequately protect Plaintiff and the members of the proposed classes from the risk of imminent and impending future harm which continues indefinitely.

C. Plaintiff Suffers the Foreseeable Consequences of Defendants' Negligence.

62. Since as early as April 2021, unauthorized entities or criminals have utilized PII obtained in the data breach, including the PII of Plaintiff, to commit actual crimes of identity theft and financial fraud.

63. On or about April 4, 2021, an unauthorized entity used Plaintiff's PII to submit a claim for Pandemic Unemployment Assistance benefits through the Pennsylvania Department of Labor & Industry, Office of Unemployment Compensation Benefits, which later received approval for a weekly benefit amount in the amount of $195.00 dollars.

64. On June 4, 2021, an unauthorized entity used Plaintiff's PII to apply for a second loan from Wells Fargo in the amount of $5,000.00 dollars.

65. On July 2, 2021, an unauthorized entity used Plaintiff's PII to apply to Wells Fargo & Company ("Wells Fargo") for a loan in the amount of $5,000.00 dollars.

66. On August 8, 2021, an unauthorized entity used Plaintiff's PII to apply to Wells Fargo for a third loan in the amount of $15,000.00 dollars.

67. On August 8, 2021, an unauthorized entity used Plaintiff's PII to open a membership and depository account with Pentagon Federal Credit Union ("PenFed").

68. On August 9, 2021, an unauthorized entity used Plaintiff's PII obtained approval from PenFed for a loan in the sum of $20,000.00 dollars.

69. On or about August 17, 2021, an unauthorized entity used Plaintiff's PII to obtain approval from GE Capital for a loan up to $5,000.00 dollars.

70. On August 18, 2021, Plaintiff reported the aforementioned acts of identity theft and financial fraud to the three major credit reporting agencies, TransUnion, Equifax, and Experian, and froze her credit.

71. Each credit agency advised Plaintiff that as a result of the severe and long-lasting ramifications of her identity theft, she should continue to freeze her credit indefinitely.

72. On or about August 18, 2021, a representative of Credtivo, an online marketplace for sourcing personal loans, contacted Plaintiff and advised her she had been approved for a loan in the sum of $5,000.00 dollars.

73. In addition to the aforementioned actual incidents of identity theft and financial fraud, Plaintiff has also suffered repeated scam robocalls to her personal telephone number, and has received numerous phishing email messages in further invasion of her personal privacy.

D. The Imminent and Impending Risk of Further Identity Theft and Financial Fraud.

74. The aforementioned actual and documented harms suffered by Plaintiff as a result of the misuse of her PII exposed in the data breach, however, do not account for the severe and long-lasting ramifications of the data breach yet to be suffered by Plaintiff or the members of the proposed classes.

75. The actual and documented misuse of Plaintiff's PII is indicative of imminent and impending identity theft or financial fraud yet to befall Plaintiff and the members of the proposed classes.

76. The ramifications of Defendants' negligent failure to secure the PII of Plaintiff and the members of the proposed classes will, in fact, continue indefinitely because once PII is stolen, the fraudulent use of that information can continue forever.

77. The data points of the stolen PII, such as dates of birth and SSNs, are persistent or permanent, and criminals who purchase or obtain the PII belonging to Plaintiff and the members of the proposed classes do not need to use the information to commit fraud immediately, but can rather use or sell the PII at any later time.

78. The persistent or permanent nature of the information compromised in the data breach limits any protective or preventative measures available to Plaintiff and the members of the proposed classes to safeguard themselves from future identity theft and financial fraud.

79. While certain information such as personal passwords or credit card numbers can be changed easily, the PII compromised in the data breach, such as dates of birth or SSNs, cannot be changed without extreme difficulty.

80. An individual cannot obtain a new SSN without significant paperwork or evidence of actual misuse. Moreover, even if a victim of identity theft changes their personal information, such as obtaining a new SSN, the absence of a prior credit history under the new number can make it more difficult for the victim to obtain credit or even rehabilitate previously damaged credit should rating agencies connect the new number to old PII.

81. Defendants themselves acknowledged in their Disclosure Letter the high certainty of severe and long-lasting ramifications from the data beach by offering Plaintiff and the members of the proposed classes a two-year subscription for credit monitoring and identity protection.

82. However, this two-year subscription is an entirely insufficient preventive measure since it does not *prevent* fraud, but rather *monitors* for it. Also, the PII exposed in the data breach

is permanently compromised, and thus exposes Plaintiff and the members of the proposed classes to identity theft and financial fraud indefinitely and beyond the meager two years of protection offered by Defendants.

83. Thus, following the expiration of the two-year subscription, Plaintiff and the members of the proposed classes will be forced to pay out-of-pocket for necessary credit monitoring and identity protection services for the rest of their lives.

E. Defendants Have a Duty to Protect the PII of Plaintiff and the Proposed Classes.

84. Based on the nature and extent of the PII maintained in its databases, Defendants knew or should have known they were an ideal target for a targeted data breach or cyberattack.

85. Defendants were also well aware that the PII of Plaintiff and the members of the proposed classes is highly sensitive and of significant value to those who would use it for wrongful purposes.

86. Defendants knew, or should have known, of the importance of adequate and reasonable security measures in maintaining the PII of Plaintiff and the members of the proposed classes based on the intrinsic value of the PII and the value Plaintiff and the members of the proposed classes would place on their PII.

87. By engaging in the gathering, possessing, storing, organizing, maintaining, and deriving of benefit from the PII belonging to Plaintiff and the members of the proposed classes, Defendants assumed legal and equitable duties to secure and protect the PII they gathered, possessed, stored, organized, maintained, and benefitted from and knew, or should have known, it was responsible for the diligent, adequate, and reasonable protection of the PII.

88. Defendants furthermore owed Plaintiff and the members of the proposed classes the duty to detect any data breach in its databases and to timely and accurately notify them of the

data breach and knew, or should have known, that timely and accurate notification would assist Plaintiff and the members of the proposed classes in protecting themselves from identity theft, financial fraud, and other misuse of their PII.

89. Defendants had the resources to invest in the necessary data security and protection measures, yet failed to undertake adequate analyses and testing of their own systems, adequate personnel training, and other data security measures to have prevented or avoided the failures that resulted in the data breach and the detection of the data breach after it initially occurred.

90. Realizing their duty with respect to PII, Defendants had already made affirmative commitments to safeguarding the data they gather and store, including the PII of Plaintiff and the member of the proposed classes, prior to the data breach.

91. With regards to the ISO ClaimSearch database, Defendants have stated the following commitment to safeguarding their data in this database:

> Because of the private nature of the information in ISO ClaimSearch®, ISO has taken precautions to restrict access and promote security. The operation of ISO ClaimSearch complies with federal and state privacy legislation as applicable.[1]

92. Defendants had also established governing policy requirements as to the privacy and security of the ISO ClaimSearch database, stating:

- Only authorized individuals within appropriate entities can access and use the data.
- Users must access and use the information in a manner consistent with laws and regulations.
- Information must be secure from damage and destruction.
- The system must have procedures to audit the access and use of database information.

[1] Privacy and Security, ISO ClaimSearch, https://www.verisk.com/insurance/products/claimsearch/privacy-and-security/ (last visited December 15, 2021).

- Users violating the policy face sanctions commensurate with the violation.[2]

93. Despite their obvious awareness of the foreseeable risk of a data breach, Defendants did not take the necessary and required minimal steps to secure the PII they gathered, possessed, stored, organized, and maintained and as a result, unauthorized entities breached and exploited Defendants' data systems and exposed the PII of Plaintiff and the members of the proposed classes.

94. Defendants breached their duties to Plaintiff and the members of the proposed classes and were otherwise negligent and reckless in failing to properly maintain and safeguard the their PII.

95. Defendants further breached their duties to Plaintiff and the members of the proposed classes in failing to provide them with timely and accurate notice of the data breach, thereby exacerbating the damages that Plaintiff and the members of the proposed classes have suffered and will continue to suffer as a result of the exposure of their PII.

96. Accordingly, as a result of Defendants' negligent failures to implement adequate and reasonable cybersecurity measures and act when required they have caused Plaintiff and the members of the proposed classes to suffer both actual harm and significant imminent or impending risk of future harm, including: (a) theft of their PII; (b) actual fraudulent activity on their financial accounts; (c) lowered credit scores resulting from credit inquires following fraudulent activity; (d) increased fraudulent phone calls and email phishing attempts; (e) costs associated with the detection and prevention of identity theft and financial fraud; (f) costs associated with time and the loss of productivity spent addressing and attempting to monitor, ameliorate, mitigate, and deal with the consequences of the data breach; (g) stress, nuisance, and annoyance from dealing with

[2] *Id.*

the consequences of the data breach; (h) imminent, impending, and increased risk of future identity theft and financial fraud posed by ill-intentioned unauthorized entities or criminals possessing their PII; (i) damages to and diminution in value of their PII; (j) the retention of the reasonable value of the PII still in Defendants' possession; and (k) the continued risk to their PII which remains in the possession of Defendants and is subject of further data breaches so long as Defendants fail to undertake appropriate and adequate cybersecurity measures.

EQUITABLE TOLLING OF STATUTES OF LIMITATIONS

97. The running of any statute of limitations has been equitably tolled by reason of Defendants' fraudulent concealment or omissions of critical information and notice of the data breach from Plaintiff and the members of the proposed classes.

98. Through affirmative misrepresentations and omissions, Defendants actively concealed from Plaintiff and the members of the proposed classes the occurrence and true extent of the data breach until providing delayed notice by the Disclosure Letter dated November 4, 2021.

99. As a result of Defendants' actions and inactions, Plaintiff and the members of the proposed classes remained unaware of the data breach, and could not have reasonably known or learned through reasonable diligence, that their PII had been exposed and that the harms set forth herein were the direct and proximate result of Defendants' acts and omissions.

CLASS ACTION ALLEGATIONS

100. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff and the members of the proposed classes seek certification of the following Nationwide Class and New York State Subclass of similarly situated persons:

NATIONWIDE CLASS

> **All natural persons residing in the United States whose personal identifiable information was compromised as a result of the data breach announced by Defendants on or about November 4, 2021, or as identified by Defendants' records relating to that data breach, or other previously undisclosed data breaches.**

101. The Nationwide Class asserts claims against Defendants for (Count I) negligence, (Count II) negligence *per se*, and (Count III) unjust enrichment. The Nationwide Class also requests (Count IV) a declaratory judgment.

102. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff and the members of proposed classes also seek certification of a New York State Subclass asserting statutory claims under (Count V) New York Gen. Bus. Law § 899-aa and (Count VI) and New York Gen. Bus. Law § 349 in addition to the claims asserted by the Nationwide class, defined as follows:

NEW YORK SUBCLASS

> **All natural persons residing in the State of New York whose personal identifiable information was compromised as a result of the data breach announced by Defendants on or about November 4, 2021, or as identified by Defendants' records relating to that data breach, or other previously undisclosed data breaches.**

103. Excluded from the Nationwide Class and New York Subclass are Defendants, any entity or entities in which Defendant have a controlling interest, Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns.

104. Also excluded from the Nationwide Class and New York Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

105. Plaintiff reserves the right to modify or amend the proposed class and subclass definitions, including, but not limited to, adding additional subclasses as necessary.

106. All members of the proposed Nationwide Class and New York Subclass are readily ascertainable in that Defendants have access to identificatory or contact information of those individuals affected by the data breach and who would be included in either class or subclass definitions, which can be used to provide notice to potential class members.

107. The Nationwide Class and New York Subclass are so numerous that joinder of all members is impracticable. The exact number and identification of proposed class members are presently unknown to Plaintiff, but upon information and belief, both the Nationwide Class and New York Subclass both include at least thousands, and potentially over millions, of individuals given the size and scope of Defendants' databases, whose personal data was conferred or entrusted to Defendants and compromised in the data breach.

108. Common questions of fact and law exist as to all members of the proposed classes, which predominate over any questions affecting only individual members to the proposed Nationwide Class and New York Subclass, including:

a. Whether Defendants failed to implement and maintain adequate and reasonable cybersecurity measures to protect the PII of Plaintiff and the members of the proposed class and subclass;

b. Whether Defendants unreasonably delayed in notifying those affected by the data breach;

c. Whether Defendants owed a duty to Plaintiff and the members of the proposed class and subclass to adequately protect their PII and to provide timely and accurate notice of the data breach to them;

d. Whether Defendants breached their duties to protect the PII of Plaintiff and the members of the proposed class and subclass by failing to provide adequate and reasonable cybersecurity and

failing to provide timely and adequate notice of the data breach to them;

e. Whether Defendants' conduct described herein was negligent;

f. Whether Defendants wrongfully or unlawfully failed to provide adequate and reasonable cybersecurity measures;

g. Whether Defendants wrongfully or unlawfully failed to inform Plaintiff and the members of the proposed class and subclass that they did not ensure that their networks or cybersecurity practices were adequate to reasonably protect their PII;

h. Whether Defendants should have notified the public, or Plaintiff and the members of the proposed class and subclass immediately upon learning of the data breach;

i. Whether Plaintiff and the members of the proposed class and subclass suffered actual injuries, including ascertainable losses, as a result of Defendants' acts or omissions;

j. Whether Plaintiff and the members of the proposed class and subclass suffered injuries, including imminent and impeding harm or enhanced risk of injury, as a result of Defendants' acts or omissions;

k. Whether Plaintiff and the members of the proposed class and subclass are entitled to recover damages, punitive damages, attorney fees, costs, and interest; and

l. Whether Plaintiff and the members of the proposed class and subclass are entitled to equitable relief, including restitution, injunctive relief, declaratory relief, or other equitable relief.

109. Plaintiff's claims are typical of the claims of the members of the proposed class and subclass in that she, like all members of the proposed class and subclass, sustained damages arising from actual harm or the imminent or impending harm arising from Defendants' acts or omissions in failing to implement and maintain adequate and reasonable cybersecurity measures to protect the PII of Plaintiff and the members of proposed class and subclass and failing to immediately notify them of the occurrence of the data breach.

110. Plaintiff is an adequate representative of the members of the proposed class and subclass because her interests do not conflict with the interests of the members of the proposed class and subclass she seeks to represent; she is represented by experienced and able counsel who have litigated numerous other fraud, negligence, complex litigation, and mass tort actions, and intend to prosecute this action vigorously for the benefit of the entire proposed class and subclass; and she and her counsel will fairly and adequately protect the interest of the members of the proposed class and subclass.

111. Furthermore, a class action is superior to other available methods for the adjudication of this litigation since individual litigation of the claims of Plaintiff and the members of the proposed class and subclass is impracticable. It would be unduly burdensome to the courts in which the many thousands of individual actions would proceed. Also, individual litigations would present a potential for inconsistent or contradictory judgments, and inevitably increase the delay and expense to all parties and the courts in resolving the legal and factual issues of these cases.

112. By contrast, the class action, as a device for the adjudication of the claims asserted herein, presents far fewer managerial difficulties while providing the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

On Behalf of Plaintiff, the Nationwide Class, and New York Subclass.

113. Plaintiff repeats, reiterates, and re-alleges each and every allegation contained in this Complaint with the same force and effect as if fully set forth herein.

114. Defendants owed a duty to Plaintiff and the members of the proposed class and subclass to exercise reasonable care in gathering, possessing, storing, organizing, and maintaining their PII and preventing it from being compromised, lost, stolen, accessed, or misused by unauthorized persons.

115. Defendants' duty to Plaintiff and the members of the proposed class and subclass included, among other things:

a. Designing, maintaining, and testing their data security systems to ensure the PII of Plaintiff and the members of the proposed class and subclass in Defendants' possession was adequately secured and protected;

b. Implementing processes that would detect a breach of Defendants' data security systems in a timely manner;

c. Timely acting upon warnings and alerts, including those generated by Defendants' own security systems, regarding intrusions to their networks; and

d. Maintaining data security measures consistent with industry standards.

116. Defendants had a common law duty to prevent foreseeable harm to Plaintiff and the members of the proposed class and subclass because they were the foreseeable and probable victims of Defendants' inadequate and unsecure data and cybersecurity practices.

117. In fact, not only was it foreseeable to Defendants that Plaintiff and the members of the proposed class and subclass would be harmed by their failure to protect their PII since criminals or hackers routinely attempt to steal such information and misuse it for nefarious purposes, but Defendants also knew their failures would more likely than not result in direct harm to Plaintiff and the members of the proposed class and subclass.

118. Defendants' duty also arose from their unique position as one of the largest aggregators of insurance claim data and PII in the world, and routinely engage in the collection of

highly sensitive information of claimants, generally without their knowledge or consent or any opportunity to "opt out" of these data collection activities.

119. Defendants' unique role within the insurance industry, which entrusted to them a tremendous responsibility to protect claimant data and PII, had placed Defendants in a critical position to protect against the harm suffered by Plaintiff and the members of the proposed class and subclass as a result of the data breach.

120. Defendants furthermore held themselves out as trusted stewards and custodians of claimant data, including the PII of Plaintiff and the members of the proposed class and subclass, and thereby assumed a duty to reasonably protect their data.

121. Defendants had a duty to safeguard the PII of Plaintiff and the members of the proposed class and subclass from a data breach, but also a duty to timely and accurately notify them of a data breach.

122. Timely and accurate notification of the data breach was required, appropriate, and necessary so that, among other things, Plaintiff and the members of the proposed class and subclass could take appropriate measures to freeze or lock their credit profiles; avoid unauthorized charges to their credit or debit card accounts; cancel or change usernames or passwords on compromised accounts; monitor their account information and credit reports for fraudulent activity; contact their banks or other financial institutions that issue their credit or debit cards; obtain credit monitoring services; and take other steps to mitigate or ameliorate the damages caused by Defendants' misconduct.

123. Defendants breached their duties owed to Plaintiff and the members of the proposed class and subclass as described above and were thus negligent by, among other things:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiff and the proposed class and subclass;

b. Failing to detect the data breach while it was ongoing;

c. Failing to maintain security systems consistent with industry standards; and

d. Failing to immediately disclose that the PII of Plaintiff and the proposed class and subclass in Defendants' possession had been or was reasonably believed to have been compromised, exposed, or stolen.

124. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and the members of the proposed class and subclass, their PII would not have been compromised.

125. As a direct and proximate result of Defendants' negligence, Plaintiff and the members of the proposed class and subclass have been injured as described herein and are entitled damages and pecuniary loss in an amount to be determined at trial. The actual and imminent or impending injuries of Plaintiff and the members of the proposed class and subclass include: (a) theft of their PII; (b) actual fraudulent activity on their financial accounts; (c) lowered credit scores resulting from credit inquires following fraudulent activity; (d) increased fraudulent phone calls and email phishing attempts; (e) costs associated with the detection and prevention of identity theft and financial fraud; (f) costs associated with time and the loss of productivity spent addressing and attempting to monitor, ameliorate, mitigate, and deal with the consequences of the data breach; (g) stress, nuisance, and annoyance from dealing with the consequences of the data breach; (h) imminent, impending, and increased risk of future identity theft and financial fraud posed by ill-intentioned unauthorized entities or criminals possessing their PII; (i) damages to and diminution in value of their PII; (j) the retention of the reasonable value of the PII still in Defendants' possession; and (k) the continued risk to their PII which remains in the possession of Defendants

and is subject of further data breaches so long as Defendants fail to undertake appropriate and adequate cybersecurity measures.

WHEREFORE, Plaintiff and the members of the proposed class and subclass demand judgment against Defendants, jointly and severally, for damages and punitive damages, together with interest, costs herein incurred, attorneys' fees and such other relief as this Court deems just and proper.

COUNT II
NEGLIGENCE *PER SE*

On Behalf of Plaintiff, the Nationwide Class, and New York Subclass.

126. Plaintiff repeats, reiterates, and re-alleges each and every allegation contained in this Complaint with the same force and effect as if fully set forth herein.

127. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Defendants in failing to use reasonable measures to protect PII. Numerous FTC publications and orders also form the basis of Defendants' duty.

128. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII, including the PII of Plaintiff and the members of the proposed class and subclass, and not complying with industry standards for data security.

129. Defendants' conduct was particularly unreasonable in its noncompliance given the nature and amount of PII it obtains and stores and the foreseeable consequences of a data breach in its data networks.

130. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

131. Plaintiff and the members of the proposed class and subclass are consumers within the class of persons that Section 5 of the FTC Act was intended to protect, and, moreover, the harm that has occurred is the type of harm the FTC Act was intended to guard against.

132. As a direct and proximate result of Defendants' negligence, Plaintiff and the members of the proposed class have been injured as described herein and are entitled damages and pecuniary loss in an amount to be determined at trial.

WHEREFORE, Plaintiff and the members of the proposed class and subclass demand judgment against Defendants, jointly and severally, for damages and punitive damages, together with interest, costs herein incurred, attorneys' fees and such other relief as this Court deems just and proper.

COUNT III
UNJUST ENRICHMENT

On Behalf of Plaintiff, the Nationwide Class, and New York Subclass.

133. Plaintiff repeats, reiterates, and re-alleges each and every allegation contained in this Complaint with the same force and effect as if fully set forth herein.

134. Plaintiff and the members of proposed class and subclass have an interest, both equitable and legal, in their PII which was gathered, possessed, stored, organized, and maintained by Defendants and ultimately compromised and exposed in the data breach.

135. The PII of Plaintiff and the members of the proposed class and subclass was initially conferred to Defendants generally by third-parties and without the knowledge or consent of Plaintiff and the members of the proposed class and subclass or the opportunity to "opt-out."

136. Defendants benefitted significantly from the conferral upon it of the PII of Plaintiff and the members of the proposed class and subclass, and by its retention and use of the PII for profit understood that they were in fact benefitted from the conferral and use of the PII.

137. Defendants also understood and appreciated that the PII of Plaintiff and the members of the proposed class and subclass was sensitive, private, and confidential information and its value depended upon Defendants maintaining its privacy, confidentiality, and security.

138. But for Defendants' willingness and commitment to maintain the privacy and confidentiality of the PII, the PII would not have been transferred to or entrusted with Defendants by third-parties.

139. Furthermore, if Defendants had disclosed or made apparent that their data security measures were inadequate, Defendants would not have been permitted to continue in operation by regulators, its shareholders, or participants in the marketplace.

140. As a result of Defendants' wrongful conduct as alleged herein, including, among other things, the failure to employ adequate data security measures; the continued gathering, possessing, storing, organizing, maintaining, and using of the PII of Plaintiff and the members of the proposed class and subclass without implementing adequate data security measures, and other conduct which facilitated the theft of that PII, Defendants have been unjustly enriched at the expense and detriment of Plaintiff and the members of the proposed class and subclass and continue to benefit from their PII while its value to Plaintiff and the members of the proposed class and subclass has been diminished.

141. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the gathering, possessing, storing, organizing, and maintaining of the PII of Plaintiff and the members of the proposed class and subclass while failing to secure that information from intrusion and theft.

142. It is inequitable for Defendants to be permitted to retain without justification the benefits they have received, and continue to receive, from Plaintiff and the members of the proposed class and subclass.

143. The benefit conferred upon, received, and enjoyed by Defendants was not conferred officiously or gratuitously by Plaintiff and the members of the proposed class and subclass, and it would be inequitable and unjust for Defendants to retain that benefit.

144. Defendants' retention of benefits from the PII of Plaintiff and the members of the proposed class and subclass is in fact unconscionable and inequitable and under the circumstances described herein constitutes unjust enrichment.

145. As a direct and proximate result of Defendants' conduct, Defendants are therefore liable to Plaintiff and the members of the proposed class and subclass for restitution in the amount of the benefit conferred upon them, including, specifically, the value to Defendants of the PII that was compromised, exposed, or stolen in the data breach and the profits Defendants received from the use of that information.

WHEREFORE, Plaintiff and the members of the proposed class and subclass demand judgment against Defendants, jointly and severally, for damages and punitive damages, together with interest, costs herein incurred, attorneys' fees and such other relief as this Court deems just and proper.

COUNT IV
DECLARATORY JUDGMENT

On Behalf of Plaintiff, the Nationwide Class, and New York Subclass.

146. Plaintiff repeats, reiterates, and re-alleges each and every allegation contained in this Complaint with the same force and effect as if fully set forth herein.

147. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief.

148. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

149. An actual controversy has arisen in the wake of the data breach described herein regarding Defendants' present and prospective common law and other duties to reasonably safeguard and secure the PII of Plaintiff and the members of the proposed class and subclass and whether Defendants are currently maintaining or implementing data security measures adequate to protect the PII of Plaintiff and the members of the proposed class and subclass from further data breaches that compromise their PII.

150. Plaintiff and the members of the proposed class and subclass allege that Defendants' data security measures remain inadequate, while Defendants allege to have taken steps to improve their data security measures to reduce the risk another data breach will ever happen again.

151. Plaintiff and the members of the proposed class and subclass however continue to suffer injury as a result of the compromise of their PII and remain at imminent and impending risk that their PII will be misused, if not already, or further compromised in the future.

152. Pursuant to its authority under the Declaratory Judgment Act, the Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to secure the PII conferred to them by third-parties and to timely notify the individuals whom the PII pertains to in the event of a data breach under common law, Section 5 of the FTC Act, and various state statutes; and

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure the PII conferred to them by third-parties.

153. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate data security measures and protocols consistent with legal and industry standards to protect the PII in their possession.

154. If an injunction is not issues, Plaintiff and the members of the proposed class and subclass will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Defendants' data systems, and the risk of another such data breach is real, immediate, impending, and substantial.

155. The hardship to Plaintiff and the members of the proposed class and subclass if the Court does not issue and injunction exceeds the hardship to Defendants if an injunction is issued.

156. Should another data breach occur, Plaintiff and the members of the proposed class and subclass will likely be subjected to substantial identify theft and financial fraud. On the other hand, the cost to Defendants in complying with an injunction by employing reasonable prospective data security measures is relatively minimal.

157. Issuance of the requested injunction will furthermore serve the public interest by preventing another such data breach, thus eliminating additional injuries that would result to Plaintiff, the member of the proposed classes, and potentially over millions of individuals whose PII would be further compromised.

WHEREFORE, Plaintiff and the members of the proposed class and subclass demand judgment against Defendants, jointly and severally, for declaratory relief, injunctive relief, damages and punitive damages, together with interest, costs herein incurred, attorneys' fees and such other relief as this Court deems just and proper.

COUNT V
INFORMATION SECURITY BREACH AND NOTIFICATION ACT
(N.Y. GEN. BUS. LAW § 899-aa)

On Behalf of the New York Subclass.

158. Plaintiff, individually, and on behalf of the New York Subclass, repeats, reiterates, and re-alleges each and every allegation contained in this Complaint with the same force and effect as if fully set forth herein.

159. Defendants are businesses that own or license computerized data that include "Personal Information" as defined by N.Y. Gen. Bus. Law § 899-aa(1)(a):

> (a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.

N.Y. Gen. Bus. Law § 899-aa(1)(a).

160. Defendants also maintain computerized data that include "Private Information," which Defendants do not own, as defined by N.Y. Gen. Bus. Law § 899-aa(1)(b):

> (b)"Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:
>
> (1) social security number;
>
> (2) driver's license number or non-driver identification card number;
>
> (3) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account;
>
> (4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or

> (5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or
>
> (ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.
>
> "Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

N.Y. Gen. Bus. Law § 899-aa(1)(b)

161. Accordingly, Defendants are subject to N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

162. The PII of Plaintiff and the members of the proposed New York Subclass that was compromised and exposed in the data breach includes "private information" covered by N.Y. Gen. Bus. Law § 899-aa(1)(b).

163. Therefore, Defendants were required to give immediate notice of the breach of security of its own data system to the owners of the private information which Defendants do not own, including Plaintiff and the members of the proposed New York Subclass, pursuant to N.Y. Gen. Bus. Law § 899-aa(3).

164. Defendants are required to accurately notify Plaintiff and the members of the proposed New York Subclass if it discovers a security breach, or receives notice of a security breach which may have compromised private information which Defendants own or license, in the most expedient time possible and without unreasonable delay, pursuant to N.Y. Gen. Bus. Law § 899-aa(2).

165. In failing to disclose the data breach in a timely and accurate manner, Defendants violated N.Y. Gen. Bus. Law § 899-aa(2) and (3).

166. As a direct and proximate result of Defendants' violations of N.Y. Gen. Bus. Law § 899-aa(2) and (3), Plaintiff and the members of the proposed New York Subclass suffered damages as described herein.

WHEREFORE, Plaintiff and the members of the proposed New York Subclass demand judgment against Defendants, jointly and severally, for declaratory relief, injunctive relief, damages and punitive damages, together with interest, costs herein incurred, attorneys' fees and such other relief as this Court deems just and proper.

COUNT V
NEW YORK GENERAL BUSINESS LAW
(N.Y. GEN. BUS. LAW § 349)

On Behalf of the New York Subclass.

167. Plaintiff, individually, and on behalf of the New York Subclass, repeats, reiterates, and re-alleges each and every allegation contained in this Complaint with the same force and effect as if fully set forth herein.

168. Defendants engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect the PII of Plaintiff and the members of the proposed New York Subclass, which was a direct and proximate cause of the data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the members of the proposed New York Subclass's private information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of Defendants' data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of the PII of Plaintiff and the members of the proposed New York Subclass by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of the PII of Plaintiff and the members of the proposed New York Subclass, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure the PII of Plaintiff and the members of the proposed New York Subclass; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of the PII of Plaintiff and the members of the proposed New York Subclass, including the duties imposed by the FTC Act, 15 U.S.C. § 45.

169. Defendants' misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of PII.

170. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded the rights of Plaintiff and the members of the proposed New York Subclass.

171. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and the members of the proposed New York Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-

monetary damages, including damages from identity theft and financial fraud; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII among other injuries described herein.

172. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including potentially over millions of New Yorkers whose PII remains in the possession of Defendants and may have been compromised in the data breach.

173. As a direct and proximate result of the above deceptive and unlawful practices and acts by Defendants, Plaintiff and the members of the proposed New York Subclass suffered substantial injury that they could not reasonably avoid.

174. As a direct and proximate result of Defendants' violations of N.Y. Gen. Bus. Law § 899-aa(2) and (3), Plaintiff and the members of the proposed New York Subclass suffered damages as described herein.

WHEREFORE, Plaintiff and the members of the proposed New York Subclass demand judgment against Defendants, jointly and severally, for declaratory relief, injunctive relief, damages and punitive damages, together with interest, costs herein incurred, attorneys' fees and such other relief as this Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of the Nationwide Class and New York Subclass, demands judgment against Defendants jointly and severally for damages to which she and all other similarly situated are entitled by law, as well as all costs of this action, interest and attorneys' fees, to the full extent of the law, including:

a. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that

Plaintiff is a proper class and subclass representative; and appoint Plaintiff's counsel as Class Counsel;

b. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

c. That the Court award Plaintiff and the Nationwide Class and New York Subclass compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

d. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

e. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

f. That Plaintiff and the Nationwide Class and New York Subclass be granted the declaratory relief sought herein;

g. That the Court award to Plaintiff and the Nationwide Class and New York Subclass all costs and disbursements of this action, along with reasonable attorneys' fees, costs and expenses;

h. That the Court award pre- and post-judgment interest at the maximum legal rate; and

i. That the Court grant all such other relief as it deems just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: December 15, 2021

Respectfully Submitted,

PARKER WAICHMAN LLP

/s/Raymond C. Silverman
Raymond C. Silverman
Jerrold S. Parker
Anthony P. Mastroianni
6 Harbor Park Drive
Port Washington, NY 11050
Phone: (516) 466-6500
Fax: (516) 466-6665
rsilverman@yourlawyer.com
jparker@yourlawyer.com
amastroianni@yourlawyer.com